



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/780,681	02/08/2001	Thomas A. Kean	19546-020200US	8254
7590	10/21/2005		EXAMINER	
Donald Daybell, Esq. ORRICK, HERRINGTON & SUTCLIFFE LLP 4 Park Plaza Suite 1600 Irvine, CA 92614-2558			SON, LINH L D	
			ART UNIT	PAPER NUMBER
			2135	
			DATE MAILED: 10/21/2005	

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/780,681	THOMAS A. KEAN	
	Examiner	Art Unit	
	Linh LD Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 08 February 2001.
- 2a) This action is **FINAL**. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1,4-25 and 28-50 is/are pending in the application.
- 4a) Of the above claim(s) 42-47 is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1,4-25,28-41 and 48-50 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)	4) <input type="checkbox"/> Interview Summary (PTO-413)
2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)	Paper No(s)/Mail Date. _____
3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____	5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)
	6) <input type="checkbox"/> Other: _____

DETAILED ACTION

- 1. This Office Action is written in responding to the Election received on 07/05/05.**
- 2. Applicant elected group I, which includes claims 1, 4-25, 28-41, and 48-50.**
- 3. Claims 2-3, and 26-27 were previously canceled.**
- 4. Claims 1, 4-25, 28-50 are pending.**

Claim Rejections - 35 USC § 112

- 5. The following is a quotation of the second paragraph of 35 U.S.C. 112:**

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. **Claims 1-17 and 22-24 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.**
7. **Claims 1 recites the limitation "a first secure bitstream" in third line from the end of the claim paragraph. There is insufficient antecedent basis for this limitation in the claim. Examiner assumes that the applicant meant, "the secured bitstream encrypted by the first key". Appropriate correction is necessary.**
8. **Claim 22 recites the limitation "the FPGA" in the 2nd lines of the claim. There is insufficient antecedent basis for this limitation in the claim. Examiner assumes that the applicant meant "the FPGA chip". Appropriate correction is necessary.**

Claim Rejections - 35 USC § 102

9. **The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:**

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

10. Claims 1, 4-5, 9, 11, 13, 25, 28, 33, 35, and 37 are rejected under 35

U.S.C. 102(e) as being anticipated by Lawman, US/6028445.

11. As per claims 1 and 25:

Lawman discloses "A method comprising: fabricating a first plurality of FPGA integrated circuits, with a first secret key embedded by way of a first mask set (Col 5 lines 39-45 and lines 20-30, user logic is the key); and "fabricating a second plurality of FPGA integrated circuits with a second secret key embedded by way of a second mask set" in (Col 5 lines 54-62, Col 7 lines 40-45, configure other portion with user logic), and "loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits (decoder or encoder) to generate a secure bitstream using the first secret key" in (Col 7 lines 25-45); "wherein the first secure bitstream will be configured properly user-configurable logic of the first plurality of FPGA integrated circuits but not the second plurality of FPGA- integrated circuits" in (Col 7 lines 25-45).

12. As per claims 4 and 28:

Lawman discloses "The method of claims 1 and 25 wherein the first plurality of FPGA integrated circuits with the first secret key are assigned to a first geographic area and the second plurality of FPGA integrated circuits with the second secret key are assigned to a second geographic area" in (Col 7 lines 35-45).

13. As per claims 5, 9, and 33:

Lawman discloses "The method of claims 1 and 25 wherein the first plurality of FPGA integrated circuits with the first secret key are fabricated in a first time period and the second plurality of FPGA integrated circuits with the second secret key are fabricated in a second time period, different from the first, time period" in (Col 7 lines 35-45).

14. As per claims 11 and 35:

Lawman discloses "The method of claims 1 and 25 wherein there are random differences between artwork of the first and second plurality of FPGA integrated circuits in addition to the different embedded secret keys" in (Col 5 lines 60-67).

15. As per claims 13 and 37:

Lawman discloses "The method of claims 1 and 25, wherein the first secret key is embedded by setting an initial state of a selection of memory cells in a device configuration memory of the FPGA integrated circuit" in (Col 5 lines 20-25).

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

17. Claims 7-8, and 31-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lawman.

18. As per claims 7 and 31:

Lawman discloses the method of claims 1 and 25. However Lawman does not teach the first plurality of FPGA integrated circuits with the first secret key are assigned exclusively to a first customer and the second key to a second customer. Nevertheless, Lawman does teach a key storage memory (Col 5 lines 10 to 11) and the configuration program logic (Col 3 lines 5-21). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art that Lawman invention does have capability to create exclusive rights for the usage of the key to a particular customer.

19. As per claims 8 and 32:

Lawman discloses the method of claims 5 and 29. However, Lawman does not teach the first time period is about the same duration as the second time period directly. Nevertheless, Lawman does teach a capability of programming the PLD to utilizing two keys at once (Col 5 lines 40-59). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art that the PLD can encrypt the bitstream at the same time period.

20. Claims 6, 10, 30 and 34, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lawman in view of Kean et al, US Patent No. 6292018B1, hereinafter “Kean” (Cited in PTO-892 dated 08/09/04).

21. As per claims 6 and 30:

Lawman discloses the method of claims 1 and 25. However, Lawman does not teach the only one mask differs between the first and second mask sets. Nevertheless, Kean does teach the one mask differs between the first and the second mask sets (Col 30 lines 33-60). Therefore, it would be obvious at the time of the invention was made for one of ordinary skill in the art to combine both teachings to switch the masking at a fast rate.

22. As per claims 10 and 34:

Lawman discloses the method of claims 6 and 30. However, Lawman does not teach the one mask is a contact mask. Nevertheless, Kean does in (Col 29 lines 2-11). Therefore, it would be obvious at the time of the invention was made for one of ordinary skill in the art to combine both teachings to switch the masking at a fast rate.

23. Claims 12, 16, 18-21, and 36, are rejected under 35 U.S.C. 103(a) as being unpatentable over Lawman in view of Erickson et al, US patent No. 6212639B1, hereinafter “Erickson” (Cited in PTO-1449 dated 10/15/01)

24. As per claims 12 and 36:

Lawman discloses “The method of claims 1 and 25”.

However, Lawman is silent on “the first and second secret keys are presented on wires of respective plurality of FPGA integrated circuits for only a limited duration”.

Nevertheless, Erickson discloses “the first and second secret keys are presented on wires of respective plurality of FPGA integrated circuits for only a limited duration” (Col 5 lines 7-17).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to modify Lawman to incorporate the renewal of the keys to provide additional security layer.

25. As per claim 16:

Lawman discloses “The method of claim 1 further comprising: loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits to generate a secure bitstream based on the first secret key” (Col 5 lines 39-45 and lines 20-30, user logic is the key).

However, Lawman does not specifically discloses “generate a secure bitstream based on the first secret key and an on-chip generated random number”.

Nevertheless, Erickson discloses a method of generating a pseudo-random key in the Programmable Logic Device (Col 4 lines 28-40).

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the teaching of Erickson with Lawman to create a double encryption layer to better secure the configuration logic data.

26. As per claim 18:

Lawman discloses a method comprising: embedding a first secret key within the artwork of an FPGA integrated circuit (decoder or de-compressor, Col 7 lines 20-45, Col 8 lines 12-63); storing second secret key within an encrypted FPGA bitstream stored in an external nonvolatile memory accessible by the FPGA (Col 2 lines 29-39, the configuration logic); decrypting the user-defined second secret key using the first secret key (Col 7 lines 20-45);

However, Lawman does not discloses "setting up a secure network link between the FPGA and a server using the user-defined second secret key"

Nevertheless, Erickson does discloses a method of setting a secure network link between the FPGA and another device, which utilizes the configuration data programs to operate as a public key cryptography circuit to establish a secure communications link in (Col 5 lines 40-60)

Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the Erickson teaching to provide a secure communication link to download the configuration logic from a configuration device or server.

27. As per claims 19-21:

Claim 18 is incorporated. Further, Lawman and Erickson disclose "the method of claim 18 further comprising: downloading an FPGA bitstream using the secure network link" in (Erickson, Col 5 lines 40-60); "encrypting the downloaded FPGA bitstream using the first secret key" in (Lawman, Col 8 lines 40-63); and storing the encrypted downloaded bitstream in the external memory (Lawman, Col 8 lines 40-63).

28. Claims 14-15, 17, and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lawman in view of Plants, US Patent no. 6560743B2 (Cited in PTO-892 dated 08/09/04).

29. As per claims 14-15, and 38:

Lawman discloses the method of claims 1 and 25. However, Lawman does not teach the first secret key is embedded by changes to a relatively large block of logic in the first plurality of FPGA integrated circuits and its value extracted using a CRC algorithm. Nevertheless, Plants discloses the "Cyclic Redundancy Checking of a Field Programmable Gate Array Having a SRAM Memory Architecture" invention, which has a CRC circuit to make sure the correct data is received (Col 2 lines 50-67 and Col 7 lines 8-16). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate Plants CRC checking method into Lawman invention to add the data and key integrity checking mechanism.

30. As per claim 17:

Lawman discloses the method of claim 1 further comprising: loading an unencrypted bitstream into one of the first plurality of FPGA integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random number (Col 4 lines 28-39). However, Lawman does not teach the secure bitstream includes a message authentication code (MAC). Nevertheless, Plants does teach the implementation of the MAC or well known in the art the "signature" to check the validity of the data stream (Col 10 lines 65-67). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate Plants CRC checking method into Lawman invention to add the data integrity checking mechanism.

Claim Rejections - 35 USC § 103

31. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

32. Claims 22-24, and 48-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lawman in view of Candelore et al, US Patent no. 6061449, hereinafter “Candelore” (Cited in PTO-1449 dated 10/15/01).

33. As per claims 22 and 48:

Lawman discloses a method comprising: storing a first secret key on an FPGA chip (See Claim 18). However, Lawman does not teach the causing of the FPGA to calculate a message authentication code (MAC) corresponding to a user design; and storing the message authentication code with bitstream information in a nonvolatile memory. Nevertheless, Candelore discloses the “Secure Processor with External Memory Using Block Chaining and Block Re-ordering” invention, which includes the generation of the MAC and storage device for keeping necessary info to receive the contents data and authentication data (Col 4 lines 45-64). Therefore, it would have been obvious at the time of the invention was made for one have ordinary skill in the art to incorporate both teaching to ensure high quality data protection.

34. As per claims 23-24 and 49:

Lawman and Candelore disclose the method of claims 22 and 48 wherein the detecting unauthorized alterations to the bitstream using the message authentication code and storing the MAC in the storage device (Candelore, Col 4 lines 45-64) the method further comprising: storing copyright messages with the bitstream information; and preventing bitstreams, which have been altered from being used to configure an FPGA (Lawman, Col 10 lines 55-60).

35. As per claim 50:

Lawman and Candelore discloses "The method of claim 48 further comprising: recording the message authentication code (Candelore, Col 4 lines 45-64) along with corresponding identification information for a product containing the FPGA (Lawman, Col 10 lines 50-60); and However, Lawman and Candelore are silent on "examining the message authentication code stored in the nonvolatile memory of a product containing a pirated FPGA design, which will enable determining the identity of the customer to whom the pirated FPGA was originally supplied using a record of MACs and corresponding product identification".

Nevertheless, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to realize that the MACs information and production information can be easily associated with a user or customer and identifiable.

Response to Arguments

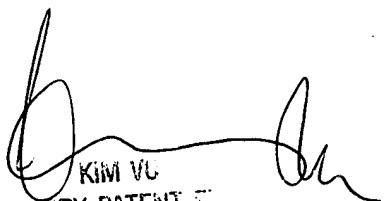
1. Applicant's arguments, see Amendment, filed 11/22/04, with respect to the rejection(s) of claim(s) 1-3, 5, 9, 11-13, 16, 25-27, 29, 33, 35, 37, and 41 under 35 USC 102(e) and Claims 4, 7, 8, 18-21, and 31-32 under 35 USC 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Lawman, Erickson, Plants, Candelore.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Linh LD Son whose telephone number is 571-272-3856. The examiner can normally be reached on 9-6 (M-F).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Linh LD Son
Examiner
Art Unit 2135



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135